

**AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS**

I, GARRETT M. GREER, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I make this affidavit in support of applications for search warrants for information associated with the following email accounts:

a. “restu.sunarto1@gmail.com” (hereinafter referred to as “**SUBJECT ACCOUNT 1**”), that is stored at premises owned, maintained, controlled, or operated by Google, Inc. (“Google”) and further described in Attachment A-1; and

b. “sunarto\_restu@hotmail.com” (hereinafter referred to as “**SUBJECT ACCOUNT 2**”), that is stored at premises owned, maintained, controlled, or operated by Microsoft, Inc. (“Microsoft”) and further described in Attachment A-2.

2. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B-1 and B-2, respectively. Upon receipt of the information described in Section I of Attachment B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1 and B-2.

**AGENT BACKGROUND**

3. I am a Special Agent (“SA”) with the Office of Export Enforcement (“OEE”), Bureau of Industry and Security (“BIS”), of the United States Department of Commerce (“DOC”), and have been since July 2019. From December 2008 through July 2019, I worked for the Department of Homeland Security as a special agent and then an intelligence research specialist. From February 2007 through December 2008, I served as a police officer in Groveland, Massachusetts. I am authorized to make arrests for violations of federal law, 50 U.S.C. § 4820.

4. I am familiar with the means by which individuals and businesses use complex procurement networks to circumvent US export law. I attended and completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC) in March 2009. At FLETC we received specialized training in various criminal investigations to include munitions and export laws. I have conducted numerous investigations that involve various techniques throughout the course of the investigations. These techniques include but are not limited to physical surveillance, technical surveillance, and various types of search warrant executions on businesses, residences, electronic mail accounts, and utilizing confidential informants in furtherance of the investigations.

**PURPOSE OF THE AFFIDAVIT**

5. Based on my training and experience and the facts as set forth in this affidavit, I believe that the targets of this investigation have committed, are committing, and will continue to commit violations of U.S. export control laws, including violations of 50 U.S.C. § 4819 (the Export Control Reform Act (ECRA)); 22 U.S.C. § 2778 (The Arms Export Control Act (AECA)) and 22 C.F.R. Part 120 (International Traffic in Arms Regulations (ITAR)) (collectively, the

“Subject Offenses”). There is also probable cause to search **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2** for evidence of the Subject Offenses listed in Attachment B.

6. I make this affidavit based on my personal knowledge derived from my participation in this investigation and upon information from the following sources, which I believe to be reliable:

- a. My training and experience investigating U.S. export control laws;
- b. Oral and written reports obtained from other federal law enforcement officers;
- c. Interviews with and documents provided by cooperating individuals and business; and
- d. Email communications.

7. The purpose of this affidavit is limited to showing that probable cause exists to support issuance of the requested search warrants. Accordingly, while this affidavit contains all the material information I am aware of that is pertinent to the requested search warrants, it does not include each and every fact known by me or other investigators concerning this investigation.

### **JURISDICTION**

8. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **STATUTORY FRAMEWORK**

9. On August 13 2018, the President signed into law the National Defense Authorization Act of 2019, which included ECRA. In part, ECRA provides permanent statutory authority for the EAR, which most recently had been operative under the International Emergency Economic Powers Act, 50 U.S.C. § 1701-1706 (“IEEPA”). Accordingly, ECRA is

the controlling statute (as the authority to promulgate export control regulations) for conduct occurring after August 13, 2018.

10. ECRA provides that “the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled.” 50 USC 4811. To that end, and like IEEPA before it, ECRA grants the President the authority to “(1) control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information, 50 USC 4812. ECRA grants to the Secretary of Commerce the authority to establish the applicable regulatory framework. 50 U.S.C. 4813.

11. ECRA allows DOC to review and control the export of certain items, including goods, software, and technologies. The Export Administration Regulations (EAR) (15 CFR parts 730-774) provide the regulatory framework as provided by the ECRA. In particular, the EAR restricts the export of items that could contribute to the military potential of other nations or that could be detrimental to United States foreign policy or national security. The EAR impose licensing and other requirements for items subject to the EAR to be lawfully exported from the United States or lawfully re-exported from one foreign destination to another.

12. The most sensitive items subject to EAR controls are identified on the Commerce Control List, 15 C.F.R. § 774, Supp. No. 1, and are categorized by Export Classification Control Numbers, each of which has export control requirements depending on the destination, end use, and end user.

13. Under ECRA, it is unlawful for any person to violate, attempt to violate, conspire to violate, or cause a violation of its provision or any regulation, order, license, or other authorization issued under ECRA. 50 U.S.C. § 4819. A person who willfully commits or willfully aids and abets these offenses is guilty of a federal crime punishable by up to a \$1,000,000 fine and 20 years' imprisonment. ECRA 50 U.S.C. § 4819.

14. The Arms Export Control Act ("AECA") authorizes the President of the United States to control the export and import of defense articles and services from the United States, and to establish and maintain a United States Munitions List ("USML") for that purpose. 22 U.S.C. § 2778.

15. Pursuant to Executive Order 11958, the President delegated the authority to regulate the export and import of defense articles and defense services to the United States Department of State. Pursuant to that authority, the Department of State promulgated the International Traffic in Arms Regulations, 22 C.F.R. §§ 120-130 ("ITAR"). The ITAR contains the USML and regulations governing exports and imports of defense articles and services.

16. The USML sets forth specific items within a twenty-one category list that are designated as defense articles or defense services. *See* 22 C.F.R. § 121.1. Items or services that are designated or controlled under any category of the USML "Any person who intends to export or to import temporarily a defense article must obtain the approval of the Directorate of Defense Trade Controls prior to the export ("DDTC"). *See* 22 C.F.R. § 123.1.

#### **PROBABLE CAUSE**

17. New England Custom Gun Service is a business located in Claremont, New Hampshire, that specializes in gunmaking, gunsmithing and firearm restoration services to the

sporting arms community. The business also sells long arms, optics and gun components. Customers of New England Custom Gun are able to purchase items online or by appointment at the business.

18. On July 16, 2019, New England Custom Gun Service received an online order for a Meostar R2-2.5-15x56 RD 4C illuminated reticle (a riflescope) from a customer identified as “Restu Sunarto,” with a shipping and billing address of 3340 A Greens Road Suite 700, Room 2269, Houston, Texas. The customer used a credit card to pay for this order. Moreover, the customer provided a phone number, 514-933-5120, and an email address, **SUBJECT ACCOUNT 2.** After the order was placed, the order status info showed that the “scope is not in stock and would take a few weeks for delivery.” In addition, when the customer placed this order, New England Custom Gun Service’s website recorded the I.P. address (xxx.xxx.xxx.187) and the referring website (Google Canada).

19. On July 16, 2019, HSI Manchester and the OEE Boston Field Office were contacted by a New England Custom Gun Service employee. The employee stated that he had just received an order for a Meopta riflescope through their website and that it raised some concerns. The employee further stated that when someone purchases a high priced scope the customer usually call and ask questions about the item, but this particular customer did not call with any questions. The employee further stated that he was concerned about the order because it was to be delivered to a warehouse in Houston, Texas, and that when they attempted to call the number that was connected to the order, they received an automated message stating that the number was not able to accept incoming calls. The employee stated that they wanted to make law enforcement aware of this order in case it was something more than just a scam attempt.

20. New England Custom Gun did not process the order right away; they informed the customer via email that the item was unavailable at the time and were currently on back order.

21. During this investigation, through open source databases, agents learned that the phone number 514-933-5120 was associated with Montreal, Quebec, Canada. Agents used online resources to identify the internet service provider for I.P. address xxx.xxx.xxx.187, and learned that Total Server Solutions L.L.C., located in Vancouver, British Columbia, Canada, owned I.P. address xxx.xxx.xxx.187.

22. On August 12, 2019, New England Custom Gun Service received another online order for another riflescope, a GPOTAC 8x24i with horseshoe reticle GPORT820, from “Restu Sunarto,” using the billing and shipping address and telephone number as the July 16<sup>th</sup> order. The customer provided **SUBJECT ACCOUNT 2** as an email account. In addition, when the customer placed this order, New England Custom Gun Service’s website recorded the I.P. address (xxx.xx.xx.111).

23. Later, agents used online resources to identify the internet service provider for I.P. address xxx.xx.xx.111, and learned that Nobis Technology Group, LLC, located in Seattle, Washington, owned I.P. address xxx.xx.xx.111.

24. In August 2019, HSI and OEE agents went to New England Custom Gun Service to interview the employee and advised him to contact the buyer. At the request of investigators, on or about August 21, 2019, New England Custom Gun Service sent the following email to the customer at **SUBJECT ACCOUNT 2**:

Hello Sir,  
I apologize for the delay on this. We did not have this scope in stock and the importer was also out.  
They tell us the scope is now in stock and available. In the meantime our credit card processing company implemented a new policy in which they ask for additional verification of the card.  
Can you please send us a picture of the card, both front and back. Once we have this we will get the order processed and the scope shipped to your location.  
I again apologize for any inconvenience this may cause. We appreciate your order and hope to have you as a future customer.  
If you have any questions, please contact me directly.

25. On or about August 21, 2019, the customer responded with the following email from **SUBJECT ACCOUNT 2**:

Hello,

Thank you for your email, It was my order 1 month ago and you have just contacted me now and asked for Verification, I appreciate your intention but was my order placed before or after the new policy appeared ?

26. After New England Custom Gun Service explained the reason for its request for credit card verification and delayed shipment for the customer's first order, on or about August 23, 2019, the user of **SUBJECT ACCOUNT 2** emailed photographs of a Citibank Visa credit card with the name "Restu Sunarto." Upon receipt of the credit card photographs, New England Custom Gun Service forwarded the photographs to federal agents.

27. OEE SA Brendan Quinlan examined the photographs and identified several areas of concern regarding the credit card. SA Quinlan has investigated access device fraud cases in the past and noted that the card did not have a chip, the location of the hologram on the front rather than the back of the card as is typical, and the hologram appeared to be a foil rather than an authentic hologram image. SA Quinlan used online resources to identify the issuing bank and determined that Citibank was not the issuing bank based on the first 6-8 digits, known as the bank identification number (BIN), of the card. Instead, the credit card's BIN corresponded with

a Visa credit card issued from Hana Bank based in the Republic of Korea. The BIN being wrong and the lack of a chip in the card led DA Quinlan to believe that the card was fraudulent.

28. In addition, upon reviewing the email exchanges between New England Custom Gun Service and **SUBJECT ACCOUNT 2**, I noted that some of the email headers included foreign-language words such as “dari,” “kepada,” and “dikirim”. Using Google translate, I determined that the language used in the header is Indonesian, and I learned that the word “dari” translates to “from,” “kepada” translates to “to,” “dikirim” translates to “shipped”.

29. Based on my training and experience, and knowledge gained during this investigation, I believe that the user of **SUBJECT ACCOUNT 2** intended to unlawfully export the two riflescopes to Canada following delivery to Houston, Texas, from Claremont, New Hampshire. My belief is based on the fact that customer provided a Canadian telephone number; the I.P. address for the first order corresponded to an internet service provider located in British Columbia, Canada; the I.P. address for the second order corresponded to an internet service provider located in Seattle, Washington, which is near Canada; the issuing bank for the credit card is not Citibank, but rather a Korean issuer; and the email headers included words in the Indonesian language. Other than the shipment address, which appears to belong to a freight forwarding company rather than an individual, there is no evidence that the actual customer is located in Houston, Texas.

30. I requested a license determination from DOC’s Office of Export Administration for the two riflescopes ordered by the user of **SUBJECT ACCOUNT 2**. According to Ronald Rolfe of the Non-Proliferation and Treaty Compliance, Nuclear and Missile Technology Division, both riflescope ordered by the user of **SUBJECT ACCOUNT 2** are classified under

ECCN 0A987.a and are controlled on the Commerce Control List (15 C.F.R. Part 774, Supplement No. 1), which means that a Firearms Conventions Import Certificate is required for license applications for firearms and related commodities, regardless of value, that are destined for member countries of the Organization of American States, of which Canada is a member.

31. In an effort to identify the destination of the two riflescopes ordered by the user of **SUBJECT ACCOUNT 2**, agents sought judicial authorization to use a tracking device in this investigation. On August 29, 2019, the Honorable Andrea K. Johnstone, U.S. Magistrate Judge for the District of New Hampshire, issued a tracking warrant for a package to be shipped from New England Custom Gun Service to “Restu Sunarto” at 3340 A Greens Road Suite 700, Room 2269, in Houston, Texas. Instead of the two riflescopes ordered by the user of **SUBJECT ACCOUNT 2**, agents placed a tracking device and various weight-bearing items to approximate the actual weight of the ordered riflescopes. The tracked package was shipped via UPS Next Day Air service on or about August 30, 2019, and UPS confirmation records show that the package was delivered on September 4, 2019.

32. On September 5, 2019, New England Custom Gun Service advised me that an individual identified as “Sunarto” called about the tracked package. “Sunarto” described opening the package and discovering cardboard and a tracking device instead of the two riflescopes ordered. “Sunarto” provided telephone number 832-630-4589. An employee of New England Custom Gun Service wrote down the name “Amine Amrouni” displayed on the caller I.D. screen.

33. At the request of the investigating agents, on September 29, 2019, special agents from OEE’s Houston Field Office traveled to Outpost SVP located at 3340 A, Green Roads,

Suite 700, Room 2269 in Houston, Texas. SA Mack described the address as a warehouse shared by three different businesses, Outpost SVC, Genuine Transportation and EP America. Specifically, SA Mack interviewed the owner of Outpost SVC, Amine Amrouni. Amrouni stated that he owned and operated Outpost SVC, whose customers use the company's U.S. address to receive shipments of goods that Outpost SVC later consolidates and forwards to another address, both foreign and domestic. During this interview, Amrouni asked SA Mack if it was ok to ship riflescopes domestically. SA Mack informed him that he had an obligation to identify if it's a routed shipment going overseas and what the intended end use was for the product. SA Mack then asked for and received consent from Amrouni to look at the shipment that Sunarto had requested to be shipped to Outpost SVC from New England Custom Gun.

34. Amrouni provided agents copies of the email communications he exchanged with Sunarto Restu over **SUBJECT ACCOUNT 1**, some of which I have summarized and excerpted below.

35. On or about September 5, 2019, after opening the tracked package from New England Custom Gun Service, Amrouni emailed the user of **SUBJECT ACCOUNT 1** and advised that it had arrived. In a series of emails exchanged on September 5, 2019, and September 6, 2019, Amrouni and the user of **SUBJECT ACCOUNT 1** discussed the contents of the tracked package. In one email, **SUBJECT ACCOUNT 1** requested a photograph of the item inside the package. Amrouni emailed two photographs and described the package as empty except for a tracking device. The user of **SUBJECT ACCOUNT 1** then instructed Amrouni to "discard or return the package (if there are no additional costs" and stated "The seller has deceived me."

36. In a series of emails exchanged between September 18, 2019, and September 23, 2019, about two packages Amrouni had received for the user of **SUBJECT ACCOUNT 1**. In response to a request for a photograph of the items, Amrouni emailed the following photographs to **SUBJECT ACCOUNT 1**:



In the same email, Amrouni asked, "This is some heavy duty stuff .. what are they sued for ? / end user?" In a later email, Amrouni asked, "I meant USED... what are they used for .. end user. (who is using them). On or about September 19, 2019, **SUBJECT ACCOUNT 1** sent the following message:

I don't know why Badrun opened my package, Instead I asked you to take a picture of my package so that there were no missing items in it.

For packages containing nightforce, Please send them to Ida Sumanuk and hold the noisy upper packages you hold in your office.

Please calculation shipping fee.

Thanks

On or about September 23, 2019, **SUBJECT ACCOUNT 1** sent the following message:

Hello.

Please consolidation my 2 packages into 1 shipping box (see the attachment) and calculate the shipping fee to the address below :

Ida Sumanuk  
3965 Bethel Rd SE, Suite 1, PMB #361  
Port Orchard  
WA ( Washington )  
98366  
USA  
360-728-2968

and for other packages, please wait because the seller has not provided a shipping address.

In response, on September 23, 2019, Amrouni wrote, “Hi Restu, remember I told you this shipment came empty? with a tracker in it?”.

37. In a series of emails exchanged between September 25, 2019, and October 1, 2019, Amrouni and the user of **SUBJECT ACCOUNT 1** discussed extra stainless steel replacement barrels that Amrouni had available for domestic sale as well as the intended end user. On September 26, 2019, the user of **SUBJECT ACCOUNT 1** wrote, “Alright I will offer it to my customers, Hopefully they are interested.” On September 30, 2019, **SUBJECT ACCOUNT 1** emailed the following offer: “They offer you 100 \$ / item and 24 \$ for you, so a total of 300 \$ for all items and a 25 \$ fee for you.”

38. On October 1, 2019, at the direction of SA Mack, Amrouni sent the following email to **SUBJECT ACCOUNT 1**:

Hi Restu,  
it will be an extra \$70 as it added some weight to it .

One question. As we face some strict laws and regulations here in America, I must ask you just for a peace of mind.

What / who is the end user of this product ( gun parts , and fire arm related items ).

Thank you

In response, **SUBJECT ACCOUNT 1** sent the following email:

Hello,

Alright I will immediately pay and wait for certainty of the items you offer and combine that item into a shipping box with another package.

My answer : All of that is an order of a rank of army general in my country, I make sure all items are not used for unlawful acts in my country, Average the item was used for hunting and tournament in a firearm community and some are sold among hunting partners. all the items that I have received from you, they immediately register to **PERBAKIN** and checked every month so as not to be misused.

Amrouni then declined to sell the replacement barrels to the user of **SUBJECT ACCOUNT 1**.

According to Amrouni and a Google search, Perbakin appears to be a shooting club located in Indonesia.

39. In addition to the assistance described above, Amrouni also provided SA Mack with two previous orders his company forwarded to Sunarto Restu on August 9, 2018 and January 17, 2019. Amrouni reported that he believed Sunarto Restu lived in either Singapore or Indonesia as Outpost SVC shipped packages to those countries at the Sunarto Restu's request. Around the times of both previous transactions, Sunarto Restu used **SUBJECT ACCOUNT 1**. He also referred to a separate email address, restusunarto131@yahoo.com.

40. On or about August 27, 2019, pursuant to 18 U.S.C. § 2703(f)(1), I sent a preservation request letter to Microsoft for **SUBJECT ACCOUNT 2**, for June 1, 2019 through August 27, 2019. Microsoft confirmed receipt of the preservation request.

41. On or about October 9, 2019, pursuant to 18 U.S.C. § 2703(f)(1), I sent a preservation request letter to Google for **SUBJECT ACCOUNT 1**, for June 1, 2019 through October 9, 2019. Google did not confirm receipt of the preservation request.

**BACKGROUND CONCERNING EMAIL**

42. In my training and experience, I have learned that Google and Microsoft provides a variety of on-line services, including email access, to the public. For example, Google allows subscribers to obtain email accounts at the domain name Gmail.com, like **SUBJECT ACCOUNT 1** listed in Attachment A-1, and Microsoft allows subscribers to obtain email accounts at the domain name Hotmail.com, like **SUBJECT ACCOUNT 2** listed in Attachment A-2. Subscribers obtain an account by registering with the email providers. During the registration process, the email provider asks subscribers to provide basic personal information. Therefore, the computers of Google and Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for subscribers) and information concerning subscribers and their use of services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

43. In my training and experience, I know that an email provider's subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the email provider. In my training and experience, evidence of who was using

an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

44. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

45. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

46. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

47. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account

access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

48. Based on the aforementioned facts, I submit that there is probable cause that the target, Restu Sunarto, has unlawfully shipped controlled items through a freight forwarding company, Outpost SVC. I believe that Sunarto utilizes this freight forwarding company in an attempt to circumvent United States law by not obtaining the proper exporting licenses prior to the items being exported via Outpost SVC. As shown above, Restu Sunarto, has used both **SUBJECT ACCOUNT 2** and **SUBJECT ACCOUNT 1** to correspond with New England Custom Gun and Outpost SVC, respectively. Accordingly, probable cause exists that evidence of this illegal conduct is present in the **SUBJECT ACCOUNT 2** and **SUBJECT ACCOUNT 1**.

49. Based on the foregoing, I request that the Court issue the proposed search warrants.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

by serving the warrant on the email providers, Google and Microsoft. Because the warrant will be served on Google and Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Garrett M. Greer  
Garret M. Greer, Special Agent  
Office of Export Enforcement  
Bureau of Industry and Security  
United States Department of Commerce

Subscribed and sworn to before me on this 8th day of November, 2019.

Andrea K. Johnstone  
Honorable Andrea K. Johnstone  
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with restu.sunarto1@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc. (“Google”), which government databases indicate, accepts service of process at 1600 Amphitheatre Parkway, Mountain View, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc. (Google).**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 9, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days (November 26, 2019) of issuance of this warrant.

**Information to be seized by the government**

All information described above in Section I that constitutes [[fruits, contraband, evidence, and instrumentalities]] of violations of 50 U.S.C. § 4819 (the Export Control Reform Act (ECRA)); 22 U.S.C. § 2778 (The Arms Export Control Act (AECA)) and 22 C.F.R. Part 120 (International Traffic in Arms Regulations (ITAR), those violations involving Restu Sunarto and occurring after October 29, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) During the course of my investigation, I believe that I have established probable cause that Restu Sunarto, has unlawfully shipped controlled items through various freight forwarding companies throughout the United States. I believe that Sunarto utilizes these freight forwarding companies in an attempt to circumvent United States law by not obtaining the proper exporting licenses prior to various controlled items being exported from the United States.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The subject of the current investigation, Restu Sunarto, is believed to have been in contact with various individuals who reside in the United States, with whom she has

used to export controlled items from the United States to Singapore and Indonesia without the proper export licenses. Some of the individuals that she may have been in contact with are as follows, but is not an all-inclusive list: Amine Amrouni, Badrun Asnawi, and Tirtawinata Suryanto.